Smart Training on Privacy and Security (expanded version)

Save to myBoK

by Sandy Bacik

There is plenty of privacy and security training to be done, and many trainers struggle to get resources from their organizations and attention from their audiences. ***Sandy Bacik****, CISSP, ISSMP, CISM, CGEIT, is a principal consultant at EnerNex and a former chief security officer. Here she offers tips on designing training that can integrate HIPAA, ARRA, and the Red Flags Rule while keeping the audience engaged.*

* * *

Privacy and security provisions in HIPAA, the American Recovery and Reinvestment Act (ARRA), and the Red Flags Rule not only affect healthcare providers, health plans, and healthcare clearinghouses, but also a wide range of vendors and contractors that provide services to healthcare organizations.

Healthcare enterprises must ensure their staff, vendors, contractors, and consultants are aware of the changes and incorporate that awareness into their everyday activities. Ultimately they have a responsibility to their customers and clients to safeguard the health information they handle.

Providing that training, however, can be a challenge. Much needs to be covered, and time and money are typically in short supply. Good planning allows trainers to design training programs that cover many regulations for multiple groups and keep the audience engaged.

Five Steps in Delivering Training

Training is the acquisition of knowledge, skills, and competencies as a result of the teaching of vocational or practical skills. Think back to a particular history lesson on Paul Revere. How did he succeed in spreading the word that “the Regulars are coming out!” on his ride to Concord? Revere focused on a single task of spreading a warning of danger. He did not mince words. Training can be based on a similar principle.

Five steps typically comprise an organizational reference training model:

1. Assess and agree on training needs
2. Create training or a development specification
3. Understand learning styles and personalities
4. Plan training and evaluation
5. Design materials and methods and deliver training

Every healthcare enterprise has a security and privacy policy architecture that guides it through both routine and anomalous activities with the information that it creates, maintains, and stores on its devices. The policy architecture documents administrative, physical, and technical safeguards that can and should be turned into training opportunities.

New and updated regulations also present training opportunities. It takes a creative mind to use in-house resources and opportunities to expand a training or awareness program.

1. Assess and Agree on Needs

The first step is to assess and agree on what training is needed. Technical and management healthcare professionals need to combine training to be effective and efficient in meeting security and privacy regulations as well as additional, internal topics within the enterprise policy architecture. All of these topics have three things in common: people, information, and technology.

People include staff members (including contractors, consultants, and volunteers), business associates, and patients or clients. This can be a pretty big audience, but each category won't require the entire training. Training topics must be assigned for each staff category.

For this article, let's focus on information security, privacy, and identity theft prevention. A possible table of priority training needs based on the above regulations may look like this:

People	Security	Privacy	Theft
Business associates	x	x	x
Consultants	x	x	x
Contractors	x	x	x
Patients or clients		x	x
Direct hires	x	x	x
Management	x	x	x
Volunteers	x	x	x

Another basic table would plot the training topics required for the enterprise's policy architecture and applicable regulations:

Regulation	Security	Privacy	Theft	Reporting
Enterprise policy architecture	x	x	x	x
HIPAA	x	x		x
ARRA	x	x		x
Red Flags Rule	x		x	x

These tables illustrate a pretty big training program, yet the training for management and direct hires can be similar; the training for business associates, contractors, consultants, and volunteers can be similar; and the patients and clients training also would be similar.

However, the topics will require some integration because, for example, information that is secured may not necessarily be private or protected from theft. As you develop the training, you need to come up with ways to relate all the training topics.

2. Create the Training Specifications

A key theme for the training program might be "We must keep information confidential, available, and accurate through people, processes, and technology." Identifying stories that combine those themes will help integrate the training and reinforce its importance. Those stories could come from the news or even a situation within the organization. Examples of cross-topic stories include:

- An executive accidently sends employee compensations to the whole enterprise-security and privacy topics
- An employee or business associate sells information about a clinic's patients-security, privacy, and identity theft topics
- A volunteer leaves a clinic computer logged in after hours and the contracted maintenance staff creates a new identity-security, privacy, and identity theft topics
- An employee returns from a vacation to find his home has been broken into and his laptop, which contains patient records, has been stolen-physical security and identity theft topics
- A consultant uses an enterprise database schema and data for developing a new application and takes the data with him when the contract ends-security and privacy topics

Many of these situations could require that affected parties be individually notified under the new federal breach notification provisions; a breach involving more than 500 records in a single state would require notification of the media. Generic stories, too, can be built to assist in developing training.

3. Identify Learning Styles

Third, you need to understand how the enterprise communicates and which methods enhance staff learning retention. Asking a few questions helps determine the enterprise's training culture. Is the training audience going to be:

- People that are **relationship-oriented, sensitive, supportive, and considerate**? They tend to make decisions based on people first and facts second. They want to answer questions such as, "How will my actions affect others?", "Have I consulted others in making my decision?", and "Who is likely to be hurt by this decision?" They prefer to learn through stories that illustrate how decisions affect others, and they want to be included in the decision-making process.
- People that are **bottom-line oriented, decisive, direct, and action-focused**? They tend to make decisions based on essential facts and little hesitation. They want to get things done and will say things such as, "Stop the whining," "Cut to the chase," and "Get to the bottom line." They want brief and direct facts focusing on tasks and results.
- People that are **thorough, logical, analytical, and factual**? They place a high value on the facts, data, and reasoned conclusions. They want to know the background and all the details, and they need enough time to consider the information before making a decision. They want to make sure they get it right the first time. They want communication done logically, sequentially, and with many details.
- People that are **fun-loving, rapid-fire, creative, and flamboyant**? They may be considered flakey because they make fast decisions and change direction frequently. They also like to rebel against too much structure. They react to testimonials and creative examples and are bored by highly technical presentations.

All four styles may be present within a single organization, even down to a small group level. A presentation with a combination of details, stories, and audience involvement assists in connecting with all communication styles. Being able to communicate to each style may not minimize the conflict or questions within a training session, but it will increase the audience's receptivity to the training.

4. Plan the Training

Having gone back to the topics within the organization's policy architecture, HIPAA, ARRA, and the Red Flags Rule, you are now ready to cover a combination of information security, privacy, identity theft, confidentiality, integrity, availability, and breach reporting topics. You have found stories that will integrate the topics and bring them to life. By considering a variety of communication styles, you can speak to the audience in their own language. Now it is time to plan the training and evaluation.

Good sources for planning can come from:

- Research, case, and field study reports
- Comparative advantage reports
- Compliance and technical reports
- Feasibility studies
- Health and safety reports
- Incident reports

If you use any of these resources, remember to offer full references for those in the audience who want to read more detail. Planning quarterly training helps keep everyone up to date on the industry and the organization.

Training can incorporate many formats and media:

- Games (including prizes or certificates)
- Reminders and helpful hints printed on wallet cards, pamphlets, newsletters, and posters
- Web sites, including links to external information
- Presentations or videos with scenarios that feature role playing

Planning for program evaluation up front will help continually improve the training as time goes on. Helpful measures include the impact on the audience, how the audience related to the material, and how behavior changed after the training.

Tracking statistics before and after the training will show improvement to management and help identify what works within the organization. It will be necessary to determine how long the training records should be kept, which should align with the organization's records retention policy.

5. Develop, Design, and Deliver: An Example

The final step is to develop, design, and deliver the training. An important element will be considering how questions will be accepted and answered. Ensure there are several mechanisms for questions included within the training.

Let's walk through one complete scenario for designing, developing, and delivering training.

- You have a goal to train in-house staff on the basics of HIPAA, ARRA, and the Red Flags Rule.
- The in-house staff attending the training have a variety of communication styles, and each session will be a mixture of styles and a mixture of staff and management.
- Everyone attending knows about the regulations but may not fully appreciate how and why the regulations apply to them.
- You have up to 90 minutes to deliver the training, give the evaluation to attendees, and answer questions.

You will need to cover the following topics:

- Information types and policy architecture
- Information confidentiality, integrity, and availability
- Security and privacy provisions
- Identity theft prevention
- Breach notification
- How the provisions affect each attendee and what each attendee needs to do

At first thought, you could prepare slides that provide the definitions, references, and what to do when something happens. Boring… Staff will sit and listen and probably walk out not remembering a thing.

Making the topics relevant and real to the organization and the people in the room will make the training more interesting, keep the audience more attentive, and improve the likelihood that the information will be retained. It also will offer varied methods of delivery and communication. For example:

- Relate why compliance is needed and how it affects the organization
- Relate how compliance works with the organization's policy architecture
- Provide examples for a home and work environment
- Give samples of the different information types involved
- Find articles in the news from the past six months that relate to the healthcare field
- Look at relevant internal situations that have or almost happened
- Make some stories generic and relate to your organization
- Create a scenario of a potential incident and have audience members do some role playing

For example, a simple story like the following covers multiple topics in an interesting way:

A patient data entry clerk is having trouble with a software application. Continually, the clerk must re-enter data because the application freezes or crashes. Someone approaches and says, "I see you are having problems. May I help?" The frustrated data entry clerk glances up and sees a badge, assumes the person is staff, and says, "Yes, sit down and I'll show you." The person with the badge inserts a USB drive into the computer, types a few commands, and says, "Try it again." The data entry clerk tries again, and everything appears to work. Within days, a news article appears that a famous person was treated at the clinic for cancer, and then a patient reports his identity has been stolen.

This simple scenario deals with security, privacy, and identity theft. Having the audience suggest solutions to prevent this from happening-and even role play to demonstrate-will enhance the training due to active participation. This type of training provides detail while also allowing the audience to see the impact on others and maybe themselves. It can be easily adapted to train contractors, consultants, business associates, and patients and clients.

Using recent events in ongoing training keeps things fresh-the same and yet different. Relating the information to real-life incidents at home and work will ensure staff retain the situations and apply appropriate actions.

This expanded version of an article published in the July 2010 issue of The Journal of AHIMA *first appeared on the* Journal *Web site..*

Article citation:
Bacik, Sandy. "Smart Training on Privacy and Security (expanded version)." *Journal of AHIMA* (April 2010): web extra.